Amendments to the Specification:

The following page and line numbers refer to the specification as originally filed, while the amendments to the paragraphs reflect changes to the substitute specification filed on March 21, 2003.

Please replace the paragraph beginning at page 5, line 7 with the following amended paragraph:

HTTPS is a web protocol developed by Netscape Communications, Inc. (Netscape) of Mountain View, California and is implemented in several browsers. The HTTPS protocol encrypts and decrypts user page requests as well as the pages that are returned by the web server. HTTPS uses Netscape's SSL as a sublayer under its regular HTTP application layer. HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP. SSL uses a key size of a predetermined number of bits (typically between 40 and 128) for the RC4 stream encryption algorithm, which is considered a minimal degree of encryption for commercial exchange.

Please replace the paragraph beginning at page 6, line 9 with the following amended paragraph:

HTTP also includes a mechanism referred to as a "cookie," which is used to maintain client side persistent data. A cookie is a token, for example, a special text file, that a web site stores on a user's hard disk so that the web site stores on a user's hard disk so that the web site can remember something about the user at a later time. Typically, a cookie records a user's preferences when using a particular site. Under HTTP, each request for a web page is independent of all previous requests. For this reason, a web page server has no memory of what pages it has sent to a user previously or anything about that user's previous visits. The cookie mechanism can allow the server to store its own file on the user's own computer. The file can be typically stored in a subdirectory of the directory used to install the browser software. The cookie subdirectory can contain cookie files for each web site visited by the user that uses

cookies. Cookies are commonly used to keep track of which banner ads a user already has encountered. This tracking can assist web sites in rotating the banner ads presented and thereby minimize repetition to the user based on a user's browser type or other information provided to the web site. In order for cookies to be used for tracking, web users, must agree to let cookies be saved on their computers by configuring their browsers to accept cookies.

Please replace the paragraphs beginning at page 7, line 7 with the following amended paragraphs:

Figs. 4A and 4B show an example of an e-commerce form 400. The information ~~form~~ for the form 400 typically includes name 405, shipping address 410, billing address 415, and credit card number 420. This information is submitted to the merchant, who then uses the information to complete the transaction using various known fulfillment and delivery mechanisms.

Navigating and completing such forms involves a great deal of repetition and associated ~~convenience~~ inconvenience to users when providing name, shipping address, billing address, and credit card data to merchants. Completing electronic forms often is a tedious and error-prone process. Furthermore, using these payment systems, customers visiting several online stores may need to re-enter their payment/address information at each online store at which they make a purchase. For many stores, shoppers additionally may need to re-enter payment information at each subsequent visit.

Please replace the paragraph beginning at page 7, line 7 with the following amended paragraph:

Client-based personal electronic wallets have been developed to relieve this burden. Client-based wallets store e-commerce information for a particular user at the machine operated by that user. When that machine interfaces with a merchant website through the Internet, e-commerce information stored in the local wallet may be transferred to the merchant. However, because client-based wallets reside on the user machine, these wallets are subject to the

B4   limitations of the machine upon which they reside. For instance, security attacks on the user

machine may be used to target the wallets residing thereon. In addition, limitations on

portability for the machine result in limitations for the wallet.

Please replace the paragraph beginning at page 9, line 11 with the following amended

paragraph:

B5   Other advantages for the user include ease of use since no additional software is required.

~~Father~~Further, as the user is not tied to a single computer, the user's information can be accessed

from any computer capable of accessing the merchant's site, regardless of location. In addition,

the security of the ~~user's~~user improves because risks associated with data sniffing on the user's

local area network and accessing storage devices attached to the user's computer can be reduced.

Please replace the paragraph beginning at page 10, line 1 with the following amended

paragraph:

B6   These techniques and methods can be generalized and applied to a variety of user

preference data, e.g., travel preferences, in addition to shipping, billing, and demographic data.

~~Implementation can~~These techniques can be implemented as a system, method, software, or

some combination thereof.

Please replace the paragraphs beginning at page 12, line 7 with the following amended

paragraphs:

B7   For instance, when merchants offer QC as a payment option and the user elects to invoke

QC, the merchant passes the order information to a pre-determined SSL-enabled QC form that is

displayed to the consumer. Payment information and shipping address can be sent from the QC

database to the QC form, and the form is confirmed, rejected or modified by the user. In this

manner, the user does not need to redundantly enter payment information for each transaction or

each merchant. Rather, the user can rely on the wallet for this information, with the user

confirming the accuracy of the information. As will be explained in greater detail below, when

the wallet includes several options for payment, shipping, etc., the consumer can establish default information, and has the ability to select desired information from among that stored.

This host-based system facilitates an integration with other merchant services as well as the surrounding wallet/passport provider environment. Because the wallet and passport are host-based, the wallet and passport can be portable, ~~update-able~~updateable, secure, and simple to setup and use.

QC can be used to share many different pieces of a user's personal information, before and during an e-commerce transaction. For instance, using QC, selected user information can be shared with a merchant server, upon a user's access to a web site or later, when performing an e-commerce transaction. More specifically, upon access to a merchant's web site, the merchant can personalize the content and services provided to the user. QC can share a variety of personal information, such as travel preferences, demographic information, food choices, and medical information. Thereafter, upon checkout, personal information of a more specific nature, generally concerning e-commerce information, can be shared. For instance, commercial information such as user name, address, and credit card information can be shared, when appropriate, to further e-commerce transactions. Each user's information can be stored in a "profile" that can be updated. This information can be stored in a proprietary or commercially available relational or object database management system (DBMS), such as provided by Oracle, Inc. or Informix, Inc.

Please replace the paragraph beginning at page 19, line 7 with the following amended paragraph:

~~Fig. 21 shows an implementation as part of one particular infrastructure of the host-to-host architecture, as described above, with the addition of a proxy 2102.~~In some implementations, a proxy server is used with the host-to-host architecture. The proxy ~~2102~~can act as an intermediary for traffic between host service computers and the Internet. The proxy ~~2102~~can perform load balancing by switching connections to the least utilized hardware for performance. The proxy ~~2102~~also contains a list of hosts that can be redirected to internal AOL

sites. The internal sites provide AOL users with a more consistent look and feel. The internal sites can also be more tightly integrated with the AOL system because they are under AOL control.

Please replace the paragraphs beginning at page 20, line 20 with the following amended paragraphs:

In response to the placeorder form, available QC information can be returned from the wallet and posted at the merchant. Default QC information can be automatically selected to eliminate the need for additional user interaction, unless editing is necessary. Alternatively, the consumer can select among available QC information, e.g., credit card, shipping address information. In either case, a subset of the sensitive QC information from the wallet can be provided to the merchant in response to the placeorder request. This subset can include enough for the consumer to confirm/select, but intentionally omits some information to avoid possible security problems, such as trojan horses. The selected subset of QC information can be posted by the QC host to the merchant site at the https://payment.aol.com/order_target_url page for future use in creating a confirmation page combining order and QC information. Fields from an exemplary form are listed on pgs. 6-7 of AOL QC Merchant Connectivity Specification, which was filed with provisional application number 60/160,874 filed October 22, 1999, which is incorporated by reference in its entirety). If the merchant can allow multiple shipping destinations for aspects of a single order, and the consumer can designate multiple destinations in the information provided by the merchant to the host, multiple posts can be made by the host to the https://payment.aol.com/order_target_url page. Each post can have the same order id, number but different information where appropriate to accomplish the consumer order.

After the consumer is redirected to the merchant site, the merchant can provide an order confirmation page displaying the order and payment data. Specifically, the merchant can generate a form that displays the selected QC info and that queries the consumer to confirm the purchase. The confirmation page posts to a designated location known to wallet host, e.g., https://payment.aol.com/confirmorder. Fields from an exemplary form are listed in Appendix C

(see list of parameters listed on p8 of AOL QC Merchant Connectivity Specification). If the merchant allows multiple shipping destinations for aspects of a single order, the consumer can designate multiple destinations in the information provided by the merchant to the host, and multiple posts can be made by the host to the https://payment.aol.com/order_target_url page with the same order id number. The merchant can generate a confirmation page for each part of the order. Generally, information is filtered before being returned to the merchant for confirmation (to prevent the merchant from obtaining enough financial information to complete the transaction until after the complete transaction is confirmed by consumer). The merchant can ~~then~~ ~~display~~then display a screen requesting confirmation of ~~shopping cart to selected credit card~~ the transaction with limited information being shown about the credit card.